

UNITED STATES DISTRICT COURT

for the
Western District of Oklahoma

AMG
5/31/24

In the Matter of the Search of
(Briefly describe the property to be searched
or identify the person by name and address)

Premises known as 1922 W Park Place, Oklahoma City,
Oklahoma 73106, the surrounding curtilage, and
any vehicles, garages, and outbuildings thereon

Case No. M-24- 476 -AMG

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property (identify the person or describe the property to be searched and give its location):

See Attachment A.

located in the Western District of Oklahoma, there is now concealed (identify the person or describe the property to be seized):

See Attachment B.

The basis for the search under Fed. R. Crim. P. 41(c) is (check one or more):

- ☒ evidence of a crime;
☒ contraband, fruits of crime, or other items illegally possessed;
☒ property designed for use, intended for use, or used in committing a crime;
☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section
18 U.S.C. § 1956(h)

Offense Description
Money Laundering Conspiracy

The application is based on these facts:

☒ Continued on the attached sheet.

☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.



Applicant's signature

Michael Adams, Special Agent, FBI

Printed name and title

Sworn to before me and signed in my presence.

Date:

5/31/24



Judge's signature

City and state: Oklahoma City, Oklahoma

Amanda Maxfield Green, U.S. Magistrate Judge

Printed name and title

and information provided to me, and other documents obtained during the course of this investigation. All of the below-described dates and times are approximate.

3. The information contained in this Affidavit is submitted for the limited purpose of establishing probable cause to secure a search warrant for 1922 W Park Place, Oklahoma City, Oklahoma 73106 (the **Subject Property**), as described further in **Attachment A** (physical description) for evidence of violations of 18 U.S.C. § 1956(h) (money laundering conspiracy), as described further in **Attachment B** (description of items to be seized). The **Subject Property** appears to be the primary residence of Jessica Guadalupe Martinez (**JESSICA**), who was recently indicted on federal money laundering charges for her role in her uncle Oscar Hernandez Flores's (Oscar) drug trafficking organization. Oscar, twice indicted in the Western District of Oklahoma, remains a fugitive in Mexico. Since this Affidavit is being submitted for the limited purpose of securing a search warrant, I have not included each and every fact known to me concerning this investigation. I have set forth only the facts that I believe are necessary to establish probable cause for the requested warrant.

BACKGROUND REGARDING DRUG AND MONEY LAUNDERING CASES

4. As discussed previously, based on my training, experience, and consultation with other seasoned investigators, I am familiar with the *modus operandi* of drug traffickers and money launderers. Based on my training and experience, as well as my participation in numerous money laundering investigations, I know the following:

- a) I am aware that money launderers frequently keep assets, records, and documents related to their criminal activity, and monies derived from the sale of drugs,

in their own residences, businesses, as well as in safe houses where they are not easily detectable by law enforcement officials conducting investigations;

b) I am aware that money launderers maintain books, records, receipts, notes, ledgers, money orders, and other papers relating to the collection and transfer of monies derived from the sale of drugs, even though such documents may be in code.

c) I am aware that the aforementioned books, records, receipts, notes, ledgers, etc., are commonly maintained where individuals have ready access to them, i.e., homes, automobiles, businesses and safe houses;

d) I am aware that money launderers will frequently keep records, notes, ledgers, contact lists, and other evidence of their criminal activity on digital devices (i.e., cellphones, computers, tablets, etc.) and that they often keep such digital devices, particularly cellphones, on their person or on the premises that they control. Further, I am aware that they will often have multiple digital devices and will frequently use more than one digital device to help conduct their criminal activity. I am also aware that they will use these digital devices to further their criminal activity through the use of digital communication, including, but not limited to, e-mail, calls, and instant messaging. Further, I am aware that money launderers will attempt to conceal the information on their digital devices that is relevant to their criminal activities through the use of encrypted applications (i.e., WhatsApp, Signal, Silent Phone) and security locks on their devices;

e) I am aware that it is common for money launderers to conceal proceeds of drug sales, and records of drug transactions, drug sources and drug customers, in secure

locations within residences, garages, storage building, safes, and safety deposit boxes for ready access, and also to conceal such items from law enforcement agencies;

f) I am aware that when drug dealers acquire large sums of proceeds from the sale of drugs, they attempt to legitimize their profits;

g) I am aware that to accomplish these goals, money launderers utilize, among other things, banks and their attendant services, securities, wire transfers, money remitter services, mobile payment services, cashier checks, money drafts, real estate companies, shell corporations, and business fronts;

h) I am aware that money launderers commonly maintain addresses or telephone numbers in books or papers which reflect names, addresses, and/or telephone numbers for their associates in the drug trafficking organization for which they are employed, even if said items may be in code;

i) I am aware that drug dealers and money launderers commonly take photographs (or cause photographs to be taken) of themselves, their associates, their property and their products or currency, and that these dealers usually maintain these photographs in their possession and at their residence; and

j) I am aware that firearms are commonly used by drug trafficking organizations to protect their inventory and currency.

PROBABLE CAUSE

5. Law enforcement first became aware of Oscar Hernandez Flores (Oscar) and the drug trafficking organization (the "DTO") described herein in 2018 during an investigation targeting the Irish Mob Gang (IMG), an Oklahoma prison gang that was trafficking drugs across

the state of Oklahoma and beyond. During the investigation, which utilized Title III wiretaps, law enforcement intercepted Oscar and identified him as one of the IMG's principal sources of supply of methamphetamine ("meth"). These IMG members and their associates were ultimately indicted and convicted. *See United States v. Velasquez*, CR-18-260-SLP. Next, from roughly 2019 to 2021, law enforcement began targeting Oscar's distribution network. During that portion of the investigation ("Phase 1") investigators uncovered a massive meth distribution network led by Oscar.

6. Phase 1 established that Oscar, who was residing in San Luis Potosi, Mexico, relied on trusted family members and confidants in Oklahoma to conduct the day-to-day operations of the DTO. Those individuals in Oklahoma distributed thousands of pounds of meth to customers of the DTO and collected millions of dollars in drug proceeds—all at Oscar's direction. The investigation also revealed that Oscar had expanded his customer base: in addition to the IMG, Oscar was supplying two other prolific, drug trafficking prison gangs that had street components, specifically the Universal Aryan Brotherhood (UAB) and the Sureños.

7. Further, aided by family members in Oklahoma, Oscar was conducting a large-scale money laundering operation to transfer drug proceeds to Mexico. Those family members included Oscar's sister Domitila Martinez (Domitila), her husband Armando Martinez (Armando), and their daughter (and Oscar's niece) Jocelyn Martinez. As part of the money laundering operation, these family members would use money remitter services, such as MoneyGram, Western Union, and Maxi, to wire drug proceeds to other family members in Mexico, who accepted these proceeds on behalf of Oscar. The investigation also established, through surveillance, interviews with cooperating defendants, and money seizures, that the

DTO members in Oklahoma City were also sending bulk drug proceeds to Mexico via vehicle.

8. As a result of Phase 1 of the investigation, federal charges were filed in the Western District of Oklahoma against more than forty persons, including Oscar, Armando, Domitila, and Jocelyn. *See United States v. Hernandez*, CR-21-76-SLP. In addition, law enforcement executed over a dozen search warrants, including at the **Subject Property** (Armando's and Domitila's residence) and 1834 NW 16th Street, Oklahoma City, Oklahoma (Jocelyn's residence). Law enforcement also made significant drug and money seizures, including over one thousand pounds of methamphetamine and more than \$1 million in U.S. currency. At the time, this coordinated effort significantly disrupted Oscar's operation. It was not until the fall of 2022, however—with the help of a newly developed confidential human source (CS1)¹—that law enforcement launched the second phase of the investigation into the DTO described herein.

9. Since phase two of the investigation launched, law enforcement has identified the same DTO, albeit with some new players, continuing to function using virtually the same

¹ CS1 was arrested by law enforcement for drug related crimes. CS1 thereafter agreed to assist law enforcement and began providing information relating to this investigation in the fall of 2022. Prior to this last arrest, CS1 had been convicted of drug related crimes in 1998 (manufacturing), 2007 (trafficking), and 2021 (possession). CS1 furnished information to law enforcement in hopes of receiving consideration for his/her most recent pending charges. CS1 has also received \$1,000 in monetary compensation to date for his/her cooperation. The information provided by CS1 has been corroborated through other investigative techniques, including physical surveillance, consensually recorded conversations, and telephone analysis. Information provided by CS1 has been reliable and I am unaware of any knowingly false information furnished by CS1. Information attributed to CS1 herein, unless otherwise noted, was obtained by CS1 through his/her personal observations or conversations with targets of this investigation and their associates.

modus operandi and money laundering methods.

10. In the fall of 2022, CS1 provided information to law enforcement regarding the distribution component of the DTO in Oklahoma City. CS1 identified an individual named “Pichi”—which law enforcement now knows is Ray Lara (Lara)—that was the primary distributor for the DTO. CS1 also indicated Lara worked at the direction of “Chibalo”—which law enforcement independently verified as Oscar, in part based on the information CS1 provided regarding Oscar’s money laundering operation. Specifically, CS1 stated Oscar had two individuals collecting drug proceeds for him via Cash App. CS1 provided these persons’ Cash Tags² as “\$CashJuanjo” and “\$JessHdz001”.

11. With that information in hand, law enforcement requested records from Block Inc.—Cash App’s parent company—related to the above listed accounts and found that they belonged to Juan Hernandez Flores (Juan) (Oscar’s brother) and Jessica Martinez (JESSICA) (Oscar’s niece), respectively. In total, law enforcement obtained records of Cash App transactions for Juan and JESSICA ending in March 2024 and beginning with the account’s inception, which was 2020 for Juan and 2015 for JESSICA. After analyzing these records in detail, law enforcement concluded that Juan and JESSICA were both collecting drug proceeds from various individuals with strong ties to either the IMG, UAB, or the Sureños.

12. For example, on May 19, 2023, Cash App records show that JESSICA received \$1,000 from a Cash App account linked to Brandy Johnson (Johnson). Johnson was identified by law enforcement as an Irish Mob associate during the FBI’s 2016 investigation. Cash App

² I know based on my training and experience that a person’s Cash Tag operates like a username.

records also show that Johnson sent a payment to Juan on April 22, 2023, that included “thanksChav” in the transaction’s subject line, which I believe, based on my training and experience, is a reference to Oscar’s moniker—“Chavalin” or “Chavalan.”³ Based on my training, experience, and knowledge of the investigation, I believe that the \$1,000 sent by JESSICA was drug proceeds, as I am aware of no other reason that JESSICA would be receiving money from Johnson, an Irish Mob associate.

13. JESSICA appears to have received another payment of drug proceeds on June 24, 2023. On this date, JESSICA received \$1,300 from a Cash App account linked to the display name “MEEK LOW”. Based on my training, experience, and knowledge of the investigation, including my familiarity with the IMG, I know that “MEEK LOW”, or “Miklo”, is an alias for Nick Roberts (Roberts), whom Oklahoma Department of Corrections records state is a validated Irish Mob member currently incarcerated at James Crabtree Correctional Center in Helena, Oklahoma. Again, I believe, based on my training and experience with this particular investigation, that the only plausible reason Roberts sent JESSICA \$1,300 was as a drug payment for Oscar.

14. These drug payments to JESSICA appear to have begun after March 2021—which coincides with when Armando, Domitila, and Jocelyn were all arrested for their roles in Oscar’s DTO. This indicated to law enforcement that Juan and JESSICA, tasked with taking over Oscar’s money laundering operation, had stepped into the roles previously held by

3. For instance, Tomas Garcia, one of Oscar’s distributors in Oklahoma, knew Oscar by this moniker.

Armando, Domitila, and Jocelyn. Based on Cash App records spanning from May 2022 to February 2024, as well as law enforcement's knowledge of the sender, law enforcement believes JESSICA has collected approximately \$65,550 in drug proceeds via Cash App.⁴ Further, as previously described, law enforcement previously identified Oscar's family members accepting bulk drug proceeds and also made significant money seizures. Based on my training, experience, and knowledge of the investigation, I believe that Oscar likely introduced CashApp, and possibly other mobile payment services, as a money laundering vehicle to limit law enforcement's ability to identify his family members receiving drug proceeds on his behalf.

15. Finally, it also appears that JESSICA, in addition to receiving drug proceeds via Cash App, has sent some of these proceeds to Oscar in Mexico via international wire: law enforcement has examined records associated with the Bank of America account linked to JESSICA's Cash App, as well as transaction records from several international money remitter businesses. Specifically, between May 2022 and October 2023, law enforcement believes JESSICA sent approximately \$51,952.35 in drug proceeds via money remitter to Oscar in Mexico, which I believe was to both conceal the nature and origin of the proceeds and promote drug trafficking. Just as with the payments from Johnson and Roberts described above, law enforcement first identified payments from senders with ties to one of the many prison gangs that Oscar's DTO has sourced during the past several years. Law enforcement then consulted

⁴ To be clear, I believe that JESSICA was likely receiving more drug proceeds than this, given the size of Oscar's operation. Importantly, the amount of proceeds collected via Cash App does not account for payments received via another mobile payment service and naturally does not account for any receipts of bulk currency.

additional records from JESSICA's Cash App, her Bank of America account, and international wire services in order to ascertain whether JESSICA subsequently sent those drug proceeds via international wire to one of Oscar's family members or associates in Mexico.⁵

16. The above-described transactions, among others, were the basis for an indictment returned by the Grand Jury in the Western District of Oklahoma on May 21, 2024, charging JESSICA and Juan with a money laundering conspiracy, in violation of 18 U.S.C. § 1956(h), and other substantive money laundering offenses.

17. Law enforcement has identified the Subject Property as JESSICA's primary residence. Law enforcement was previously familiar with the Subject Property, which was subject to criminal forfeiture as a result of the FBI investigation in 2020 and 2021. As part of their plea agreements with the United States, both JESSICA's father (Armando) and her mother (Domitila) forfeited and/or abandoned all right, title, and interest to the Subject Property. Apparently in connection to those forfeiture proceedings, on approximately May 6, 2024, records with the Oklahoma County Assessor were updated to reflect the United States's title to the property. Nevertheless, JESSICA appears to still be living at the Subject Property based on her cellphone's location data, recently obtained via court authorization. Those records establish that from May 1 to May 28, 2024, JESSICA stayed at the Subject Property approximately 24 times. Law enforcement, which has a surveillance camera fixated on the

⁵ Further, based on my training, experience, and knowledge of the investigation, I believe these wire transfers were sent to family members of Oscar's, rather than Oscar, to conceal the fact they were drug proceeds. Given that Oscar is no doubt aware he has been twice indicted in the Western District of Oklahoma, he likely recognizes that transfers listing him as the recipient would raise law enforcement's suspicions.

Subject Property, has observed a female, arriving at and departing from the **Subject Property**, in a vehicle registered to **JESSICA**. All of this leads me to conclude that **JESSICA**'s primary residence is the **Subject Property**.

18. Based on my training and experience, I know that the primary residence of a money launder is the most common place to find evidence of crimes. I believe this for many reasons. First, I know that a money launder's primary residence is the most likely place to find a launderer's cellphone, assuming it is not on the launderer's person. I believe that **JESSICA**'s cell phone will undoubtedly contain evidence of her crimes given that Oscar's customers are using mobile payment applications such as Cash App to pay **JESSICA**. I also know that cellphones often contain mobile banking applications which contain information related to transactions involving the person's bank account. Here, records obtained by law enforcement establish that **JESSICA** has linked her Bank of America account and Cash App account, further leading me to believe that her cellphone will contain evidence of her crimes in the form of information pertaining to credits and debits for the account. I also believe based on my training and experience that law enforcement will likely recover other evidence at the **Subject Property**, such as receipts for transactions, banking statements, contact information for co-conspirators, notes/ledgers, dominion and control items, and bulk cash. And I believe, based on my training and experience, that some of the above-described evidence may be physical or digital in nature, *i.e.*, found on electronic devices such as cell phones and computers. In short, the investigation described herein leads me to believe that the **Subject Property** will contain evidence of the DTO's crimes, specifically evidence of violations of 18 U.S.C. § 1956(h).

HOURS OF EXECUTION

19. Your affiant is seeking authorization to execute the search warrant sought herein between the hours of 5 a.m. and 10 p.m., rather than during the standard window of 6 a.m. to 10 p.m. In conjunction with the application for a search warrant for the **Subject Property**, law enforcement is also applying for a search warrant for 1900 NW 11th St., Oklahoma City, Oklahoma—Juan’s primary residence—and is seeking authorization to execute that search warrant as early as 5 a.m. due to Juan typically leaving his residence between 5 a.m. and 6 a.m. Law enforcement is seeking the same authorization here, allowing them to execute the search warrant between 5 a.m. and 6 a.m. Law enforcement is concerned about **JESSICA**’s potential flight from prosecution or destruction of evidence should she somehow receive notice about the search warrant at Juan’s residence, his arrest warrant, or her arrest warrant. The **Subject Property** is one street south and approximately .1 miles away from Juan’s residence, leading law enforcement to believe that there is a considerable possibility that she could learn about the search warrant and accompanying arrest warrants and flee or destroy evidence prior to 6 a.m.

COMPUTERS, ELECTRONIC STORAGE, AND FORENSIC ANALYSIS

20. As described above and in **Attachment B**, this application seeks permission to search for records that might be found on the **Subject Property**, in whatever form they are found. One form in which the records might be found is data stored on a computer’s hard drive or other storage media. Thus, the warrant applied for would authorize the seizure of electronic storage media or, potentially, the copying of electronically stored information, all under Rule 41(e)(2)(B), that law enforcement reasonably believes belongs to and/or has been used by **JESSICA**.

21. *Probable cause.* I submit that if a computer or storage medium is found on the **Subject Property** and law enforcement has reason to believe that it belongs to and/or has been used by **JESSICA**, there is probable cause to believe those records will be stored on that computer or storage medium, for at least the following reasons:

- a. Based on my knowledge, training, and experience, I know that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person “deletes” a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.
- b. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the storage medium that is not currently being used by an active file—for long periods of time before they are overwritten. In addition, a computer’s operating system may also keep a record of deleted data in a “swap” or “recovery” file.
- c. Wholly apart from user-generated files, computer storage media—in particular, computers’ internal hard drives—contain electronic evidence of how a computer has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating system or application operation, file

system data structures, and virtual memory “swap” or paging files. Computer users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.

- d. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or “cache.”

22. *Forensic evidence.* As further described in **Attachment B**, this application seeks permission to locate not only computer files that might serve as direct evidence of the crimes described on the warrant, but also for forensic electronic evidence that establishes how computers were used, the purpose of their use, who used them, and when. There is probable cause to believe that this forensic electronic evidence will be on any storage medium in the **Subject Property** because:

- a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, e-mail programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer was in use. Computer file

systems can record information about the dates files were created and the sequence in which they were created, although this information can later be falsified.

- b. As explained herein, information stored within a computer and other electronic storage media may provide crucial evidence of the “who, what, why, when, where, and how” of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, information stored within a computer or storage media can indicate who has used or controlled the computer or storage media. Additionally, some information stored within a computer or electronic storage media may provide crucial evidence relating to the physical location of other evidence and the suspect. For example, images stored on a computer may both show a particular location and have geolocation information incorporated into its file data. Such file data typically also contains information indicating when the file or image was created. The existence of such image files, along with external device connection logs, may also indicate the presence of additional electronic storage media (e.g., a digital camera or cellular phone with an incorporated camera). The geographic and timeline information described herein may either inculcate or exculpate the computer user. Last, information stored within a computer may provide relevant insight into the computer user’s state of mind as it relates to the offense under investigation. For example, information within the computer may

indicate the owner's motive and intent to commit a crime (e.g., internet searches indicating criminal planning), or consciousness of guilt (e.g., running a "wiping" program to destroy evidence on the computer or password protecting/encrypting such evidence in an effort to conceal it from law enforcement).

- c. A person with appropriate familiarity with how a computer works can, after examining this forensic evidence in its proper context, draw conclusions about how computers were used, the purpose of their use, who used them, and when.
- d. The process of identifying the exact files, blocks, registry entries, logs, or other forms of forensic evidence on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. While it is possible to specify in advance the records to be sought, computer evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

23. *Necessity of seizing or copying entire computers or storage media.* In most cases, a thorough search of a premises for information that might be stored on storage media often requires the seizure of the physical storage media and later off-site review consistent with the warrant. In lieu of removing storage media from the premises, it is sometimes possible to make an image copy of storage media. Generally speaking, imaging is the taking of a complete electronic picture of the computer's data, including all hidden sectors and deleted files. Either

seizure or imaging is often necessary to ensure the accuracy and completeness of data recorded on the storage media, and to prevent the loss of the data either from accidental or intentional destruction. This is true because of the following:

- a. The time required for an examination. As noted above, not all evidence takes the form of documents and files that can be easily viewed on site. Analyzing evidence of how a computer has been used, what it has been used for, and who has used it requires considerable time, and taking that much time on premises could be unreasonable. As explained above, because the warrant calls for forensic electronic evidence, it is exceedingly likely that it will be necessary to thoroughly examine storage media to obtain evidence. Storage media can store a large volume of information. Reviewing that information for things described in the warrant can take weeks or months, depending on the volume of data stored, and would be impractical and invasive to attempt on-site.
- b. Technical requirements. Computers can be configured in several different ways, featuring a variety of different operating systems, application software, and configurations. Therefore, searching them sometimes requires tools or knowledge that might not be present on the search site. The vast array of computer hardware and software available makes it difficult to know before a search what tools or knowledge will be required to analyze the system and its data on the Premises. However, taking the storage media off-site and reviewing it in a controlled environment will allow its examination with the

proper tools and knowledge.

- c. Variety of forms of electronic media. Records sought under this warrant could be stored in a variety of storage media formats that may require off-site reviewing with specialized forensic tools.

24. *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit seizing, imaging, or otherwise copying storage media that reasonably appear to contain some or all of the evidence described in the warrant and would authorize a later review of the media or information consistent with the warrant. The later review may require techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of a hard drive to human inspection in order to determine whether it is evidence described by the warrant.

25. As with any search warrant, I expect that this warrant will be executed reasonably. Reasonable execution will likely involve conducting an investigation on the scene of what computers, or storage media, must be seized or copied, and what computers or storage media need not be seized or copied. Where appropriate, officers will copy data, rather than physically seize computers, to reduce the extent of disruption. If seizure must take place, after inspecting the computers, it is determined that some or all of this equipment is no longer necessary to retrieve and preserve the evidence, the government will return it.

**INFORMATION PERTAINING TO UNLOCKING ELECTRONIC
DEVICES WITH BIOMETRIC FEATURES**

26. The warrant I am applying for would permit law enforcement to obtain from JESSICA the display of physical biometric characteristics (such as fingerprint, thumbprint, or

facial characteristics) in order to unlock devices subject to search and seizure pursuant to this warrant. I seek this authority based on the following.

27. I know from my training and experience, as well as from information found in publicly available materials published by device manufacturers, that many electronic devices, particularly newer mobile devices and laptops, offer their users the ability to unlock the device through biometric features in lieu of a numeric or alphanumeric passcode or password. These biometric features include fingerprint scanners and facial recognition features. Some devices offer a combination of these biometric features, and the user of such devices can select which features they would like to utilize.

28. If a device is equipped with a fingerprint scanner, a user may enable the ability to unlock the device through his or her fingerprints. If a device is equipped with a facial recognition feature, a user may enable the ability to unlock the device through his or her face. The device can then be unlocked if the camera detects a face with characteristics that match those of the registered face.

29. In my training and experience, users of electronic devices often enable the aforementioned biometric features because they are considered to be a more convenient way to unlock a device than by entering a numeric or alphanumeric passcode or password. Moreover, in some instances, biometric features are considered to be a more secure way to protect a device's contents. This is particularly true when the users of a device are engaged in criminal activities and thus have a heightened concern about securing the contents of a device.

30. As discussed in this affidavit, based on my training and experience I believe that one or more digital devices will be found during the search. The passcode or password that

would unlock the device(s) subject to search under this warrant is not known to law enforcement. Thus, law enforcement personnel may not otherwise be able to access the data contained within the device(s), making the use of biometric features necessary to the execution of the search authorized by this warrant.

31. I also know from my training and experience, as well as from information found in publicly available materials including those published by device manufacturers, that biometric features will not unlock a device in some circumstances even if such features are enabled. This can occur when a device has been restarted, inactive, or has not been unlocked for a certain period of time. Thus, in the event law enforcement personnel encounter a locked device equipped with biometric features, the opportunity to unlock the device through a biometric feature may exist for only a short time.


32. In my training and experience, the person who is in possession of a device or has the device among his or her belongings at the time the device is found is likely a user of the device. However, in my training and experience, that person may not be the only user of the device whose physical characteristics are among those that will unlock the device via biometric features, and it is also possible that the person in whose possession the device is found is not actually a user of that device at all. Furthermore, in my training and experience, I know that in some cases it may not be possible to know with certainty who is the user of a given device, such as if the device is found in a common area of a premises without any identifying information on the exterior of the device. Thus, it will likely be necessary for law enforcement to have the ability to require JESSICA to unlock the device using biometric features in the same manner as discussed above.

33. Due to the foregoing, if law enforcement personnel encounter a device that is subject to search and seizure pursuant to this warrant and may be unlocked using one of the aforementioned biometric features, the warrant I am applying for would permit law enforcement personnel to (1) press or swipe JESSICA's fingers (including thumbs) to the fingerprint scanner of any device law enforcement reasonably believes her to be a user of and (2) hold the device in front of JESSICA's face and activate the facial recognition feature, for the purpose of attempting to unlock the device in order to search its contents as authorized by this warrant.

CONCLUSION

34. Based on the foregoing, I respectfully submit that there is probable cause to believe that evidence relating to violations of 18 U.S.C. § 1956(h) will be found at the **Subject Property**. I therefore respectfully request issuance of search warrants for the **Subject Property** (as set forth in **Attachment A**) based on the above-mentioned facts.

FURTHER, YOUR AFFIANT SAYETH NOT.



MICHAEL ADAMS
Special Agent
Federal Bureau of Investigation

Sworn to and subscribed before me this 31st day of May, 2024.



AMANDA MAXFIELD GREEN
United States Magistrate Judge

Attachment A

ADDRESS TO BE SEARCHED
(The Subject Property)



Description:

The **Subject Property** is located at 1922 W Park Place, Oklahoma City, Oklahoma 73106, and is a single-family residence in Oklahoma County, Oklahoma. The **Subject Property** sits on the south side of the 1900 block of W Park Place between N Kentucky Avenue and N Virginia Avenue. The **Subject Property** is a tan, one-story residence, with red trim, a white front door and a gray shingled roof. The front door faces north with a concrete walkway extending to the sidewalk. The east side of the property has a concrete shared driveway with the neighbor to the east. The property displays faint “1922” numbering on a structural column.

Attachment B

ITEMS TO BE SEIZED

The items to be seized are evidence, contraband, fruits, or instrumentalities of violations of 18 U.S.C. § 1956(h) (Money Laundering):

1. Documents, records, or materials related to the distribution of illegal drugs, including, but not limited to: ledgers, address books, telephone books, telephone bills, telephone records, rent receipts, rental car agreements, mini-storage receipts, cellular telephone agreements, pager rental agreements, bills and receipts related to cellular telephones and pagers, and any property and/or U.S. currency being proceeds of or related to the distribution of illegal narcotics. Also ledgers containing quantity of narcotics possessed, ledgers of money owed to the suspects for narcotics they have provided to co-conspirators, ledgers of money owed by the suspects to their suppliers, transportation and distribution instructions for the narcotics being sold, and other types of documentation regarding the sale of narcotics.
2. Financial documents evidencing the illegal distribution of controlled substances, including, but not limited to: bank statements, bank deposit slips, canceled checks, money orders, money order receipts, wire transfer receipts, stored value cards, handwritten notes depicting monies owed for illegal controlled substances, documents showing purported income, and any other evidence showing monetary records of the illegal distribution of controlled substances.
3. Documents, records, or materials related to the laundering of money, including, but not limited to: wire transfer receipts, bank deposit slips, bank withdraw slips, money order receipts, records detailing the purchase of property, items which show control of real property placed in nominee names such as utility payment records, property tax payment records, key to real property, receipts from payment of insurance premiums paid on residences/vehicle.

4. The fruits and proceeds of the illegal distribution of controlled substances, including, but not limited to: large amounts of currency, financial instruments and other items of value showing the spending of large sums of money made from engaging in the illegal distribution of controlled substances, or other illegal activities.
5. Any digital device used to facilitate the above-listed violations or containing evidence falling within the scope of the foregoing categories of items to be seized, and forensic copies thereof.
 - a. With respect to any digital device used to facilitate the above-listed violations or containing evidence falling within the scope of the foregoing categories of items to be seized:
 - i. evidence of who used, owned, or controlled the device at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, e-mail, e-mail contacts, chat and instant messaging logs, photographs, and correspondence;
 - ii. evidence of the presence or absence of software that would allow others to control the device, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;
 - iii. evidence of the attachment of other devices;

- iv. evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the device;
 - v. evidence of the times the device was used;
 - vi. passwords, encryption keys, and other access devices that may be necessary to access the device;
 - vii. applications, utility programs, compilers, interpreters, or other software, as well as documentation and manuals, that may be necessary to access the device or to conduct a forensic examination of it;
 - viii. records of or information about Internet Protocol addresses used by the device;
 - ix. records of or information about the device's Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses.
- b. As used herein, the terms "records," "documents," "programs," "applications," and "materials" include records, documents, programs, applications, and materials created, modified, or stored in any form, including in digital form on any digital device and any forensic copies thereof.

- c. As used herein, the term “digital device” includes any electronic system or device capable of storing or processing data in digital form, including central processing units; desktop, laptop, notebook, and tablet computers; personal digital assistants; wireless communication devices, such as telephone paging devices, beepers, cellphones, mobile telephones, and smart phones; digital cameras; peripheral input/output devices, such as keyboards, printers, scanners, plotters, monitors, and drives intended for removable media; related communications devices, such as modems, routers, cables, and connections; storage media, such as hard disk drives, floppy disks, memory cards, optical disks, and magnetic tapes used to store digital data (excluding analog tapes such as VHS); and security devices.
- 6. Items which tend to show dominion and control of the property searched, including, but not limited to, utility bills, telephone bills, correspondence, rental agreements, property tax payment records, receipt from the payment of insurance premiums on the residence, and other identification documents.
- 7. During the execution of the search of the **Subject Property** described in Attachment A, law enforcement personnel are authorized to (1) press or swipe the fingers (including thumbs) of Jessica Guadalupe Martinez to the fingerprint scanner of any device law enforcement reasonably believes her to be a user of and (2) hold a device found at the premises in front of Jessica Guadalupe Martinez’s face and activate the facial recognition feature, for the purpose of attempting to unlock the device in order to search the contents as authorized by this warrant.